CLAIMS

1. Method for protecting a portable object against denial of service type attacks, said portable object comprising a memory where at least one credential is stored, each credential being associated with a service, the method comprises the steps of :

- verifying that the entity requesting a service is an authorized entity for accessing the service, based on an algorithm involving the credential,
- delivering the requested service only when the verification step succeeded,
- blocking the credential associated with the service after a certain number of verification step failed,

wherein, when the verification step failed, the method further comprises the steps of :

- waiting during a duration before allowing a new verification step.

2. Method for protecting a portable object against denial of service type attacks as recited in claim 1, wherein the waiting duration is constant for each failed verification step.

3. Method for protecting a portable object against denial of service type attacks as recited in claim 1, wherein the waiting duration is variable for each failed verification step.

4. Method for protecting a portable object against denial of service type attacks as recited in one of the previous claims, wherein the waiting duration is equal to zero for a first predetermined number of failed verification step, and the waiting duration is greater than zero for a second predetermined number of failed verification step.

5. Method for protecting a portable object against denial of service type attacks as recited in one of the previous claims, wherein the step of waiting during a duration is resumed in case said step is interrupted before the duration has elapsed.

6. Method for protecting a portable object against denial of service type attacks as recited in claim 1, wherein said credential is a personal identification number or a key or a code.

7. Method for protecting a portable object against denial of service type attacks as recited in claim 1, wherein said entity is a user or a terminal or a server or an application.

8. Method for protecting a portable object against denial of service type attacks as recited in one of the previous claims, wherein the method further comprises the steps of :

- decrementing a counter associated with the at least one credential each time a verification step is performed, said counter having values ranging between an initial value and a credential blocking value,
- resetting the counters to the initial value when the verification step succeed,

and, when the counter has reached an intermediate value, the method further comprises the steps of :

- waiting during a duration when verification step failed,
- blocking the credential when the counter reaches the credential blocking value.

9. Method for protecting a portable object against denial of service type attacks as recited in one of the claims 1 to 7, wherein the method further comprises the steps of :

- decrementing a first counter associated with the at least one credential each time a verification step is performed, said first counter having values ranging between a first initial value and an intermediate value,

and, when the first counter has reached the intermediate value, the method further comprises the steps of :

- decrementing a second counter associated with the first counter, said second counter having values ranging between a second initial value and a credential blocking value,
- resetting the first counter to the first initial value and the second counter to the second initial value when verification step succeed,

- waiting during a duration when verification step failed,
- blocking the credential when the second counter reaches the credential blocking value.

10. Method for protecting a portable object against denial of service type attacks as recited in one of the previous claims, wherein, when verification step failed, the step of waiting during a determined duration is implemented by a waiting loop mechanism.

11. Method for protecting a portable object against denial of service type attacks as recited in claim 8, wherein the decrementing step of the counter or the first counter or the second counter are performed before the verification step.

12. Method for protecting a portable object against denial of service type attacks as recited in claim 8, wherein the decrementing step of the counter or the first counter or the second counter are performed after the verification step.

13. Portable object, in particular a smart-card, comprises :
- a memory where at least one credential is stored, each credential being associated with a service, said credential being used to verify that the entity requesting a service is an authorized entity for accessing the service,
- a counter associated with the at least one credential which is decremented each time a verification that the entity requesting a service is an authorized entity for accessing the service failed, said counter having values ranging between an initial value and a credential blocking value, said counter being reset to the initial value when verification succeed,
wherein said portable object further comprises :
- a waiting loop mechanism which is activated when the counter has reached a intermediate value and each time a verification failed.

14. Portable object, as recited in the previous claim, wherein the counter comprises a first and a second counter, the first counter associated with the at least one credential being decremented each time a verification that the entity requesting a service is an authorized entity for accessing the service failed, said

first counter having values ranging between a first initial value and an intermediate value, the second counter being decremented when the first counter has reached the intermediate value and each time a verification that the entity requesting a service is an authorized entity for accessing the service failed, said second counter having values ranging between a second initial value and a credential blocking value.

15. Portable object, as recited in one of the claims 13 to 14, wherein the waiting loop mechanism comprises a loop flag used to resume the step of waiting during a duration performed by the waiting loop mechanism in case said step is interrupted before the duration has elapsed.

16. A computer program product comprising a computer readable medium, having thereon computer program code means, when said program is loaded into the memory of the portable object, to make the portable object execute the method for protecting said portable object against denial of service type attacks as recited in any of the claims 1 to 12.